Building an effective compliance risk assessment programme for a financial institution

Stephanie Nicolas* and Paul V. May

Received: 20th January, 2017

*WilmerHale, 1875 Pennsylvania Avenue NW, Washington, DC 20006, USA;
Tel: +1 202 663 6825; Fax: +1 202 663 6363; E-mail: stephanie.nicolas@wilmerhale.com

Stephanie Nicolas *is a partner in WilmerHale's Securities Department and a member of the Broker-Dealer Compliance & Regulation Group. Ms Nicolas has extensive experience handling a broad range of regulatory and enforcement issues and conducting compliance reviews and audits. She works with major investment banks and other financial institutions to develop policies and procedures for a range of activities, including regulatory reporting, supervision, information barriers and surveillance, equity and debt research, conflicts, capital markets, and trading and sales practice issues. Ms Nicolas received her Juris Doctor,* magna cum laude, *from Georgetown University Law Center, 1999 and her BA from Brown University, 1994.*

Paul V. May *is the Chief Compliance Officer of ABN AMRO Securities (USA) LLC and its New York affiliates. Previously, he was a compliance officer and regulatory counsel at RBC Capital Markets, ICAP, and Cowen and Company. Paul served as an attorney at the Securities and Exchange Commission Enforcement Division from 1990 to 1995 and then at Kelley Drye & Warren and at Steere & May, providing broker dealer regulatory guidance and representation to firms and individuals in securities law matters. He is a graduate of the College of the Holy Cross and Brooklyn Law School.*

ABSTRACT

A Compliance Risk Assessment programme can be a meaningful, utilitarian and genuinely beneficial risk identification and management tool. This paper outlines some key elements and practical considerations for conducting a CRA. By better identifying compliance risks and managing the drivers of these risks and behaviour, a CRA not only helps firms to reduce the occurrence of conduct events, but also enhances the way that firms do business.

Keywords: compliance risk assessment(s), compliance assessment(s), conduct risk, risk assessment(s), inherent risk(s), residual risk(s)

Stephanie Nicolas

Paul V. May

INTRODUCTION

By now, at the beginning of 2017, the components of a compliance risk assessment (CRA) programme, virtually unheard of just over a decade ago, are ubiquitous. Inherent risks are identified, controls to mitigate those risks are listed and the resulting residual risk calculations are coded as high, medium or low in terms of potential financial, regulatory and public reputational damage to the entity. The resulting cycle of enhanced controls to address identified residual risks are reflected in new assessments, while newly added or discovered risks take their place at the top of the grid.

Companies just starting down the risk assessment path, or those in the early stages, face a unique opportunity to benefit from the growing pains of pioneer institutions to build a meaningful, utilitarian and genuinely beneficial risk identification and

Journal of Securities Operations & Custody
Vol. 9, No. 3, pp. 215–224

management tool. Those with established risk assessment programmes may find this an opportune time to critically evaluate these programmes to incorporate lessons learned. As a mechanism that will likely survive in some form for the life of the enterprise, this opportunity to build a strong foundational programme is indeed rare and one that, if seized upon with appropriate attention, can escape the fate of painful compliance reviews and instead become a critical scale by which to assess and address potential pitfalls before they come to damaging fruition. Our purpose here is to offer suggestions gleaned from early CRA battlefields that may help to guide the enterprise towards implementation of an effective risk management tool and overcome expected resistance from first-line businesses. While CRAs may be an expected fixture for large financial institutions, any institution that is engaged in the securities or financial markets — regardless of its size — may benefit from an effective CRA programme that mitigates regulatory exposure, costly penalties and fines, and reputational harm.

This paper first explores the regulatory backdrop for implementing CRAs, with a focus on the expectations of US regulators and authorities. Next, this paper provides practical guidance for developing a CRA and the timing of the CRA. Finally, this paper highlights a compliance risk area that, increasingly, contributes to multi-million and multi-billion dollar losses and fines and incalculable reputational damage: conduct risk — and how financial service entities ('firms') may incorporate conduct risk in their CRAs.

REGULATORY BACKDROP FOR IMPLEMENTING CRAs

In general, compliance risk assessment is a process that (1) identifies the major inherent risks within a business line or legal entity; (2) analyses any processes and procedures that are practiced by the institution to control and/or mitigate those risks; and (3) based on this analysis, produces a measurement of the residual risks that are posed to the institution.[1] The primary purpose of a compliance risk assessment is to identify areas of significant risk and where controls are needed to mitigate risk. The CRA provides a framework to enable users (eg business management and risk and compliance professionals) to formally assess the overall compliance risk associated with a particular desk, business division, legal framework, region or other applicable area.

The US banking regulators have articulated their expectations for 'compliance risk assessments' in various regulatory guidance. The seminal guidance is articulated in a 2008 Federal Reserve Supervisory Letter.[2] This supervisory letter sets forth the Federal Reserve's general expectations regarding effective firm-wide compliance risk management programmes and oversight at large, complex banking organisations. In particular, this letter instructs firms that risk assessments should be based upon firm-wide standards that establish the method for, and criteria to be utilised in, assessing risk throughout the organisation. Risk assessments should take into consideration both the risk inherent in the activity and the strength and effectiveness of controls designed to mitigate the risk.[3] Moreover, the processes established for managing compliance risk on a firm-wide basis should be formalised in a compliance programme that establishes the framework for identifying, assessing, controlling, measuring, monitoring and reporting compliance risks across the organisation, and for providing compliance training throughout the organisation.[4]

Similarly, the US Consumer Financial Protection Bureau (CFPB) expects regulated entities to have an effective 'compliance management system.' Each CFPB examination will include review and testing of components of the supervised entity's

compliance management system.[5] The US Commodity Futures Trading Commission (CFTC), which (with the implementation of Dodd Frank regulations and pending possible regulatory rollbacks) is increasingly involved in regulating financial services firms, requires certain regulated entities to furnish an annual report addressing the registrant's compliance activities.

While the securities regulators do not use the term 'compliance risk assessment' in their rules and regulations, there is an expectation that securities firms will conduct risk assessments and the US Securities and Exchange Commission (SEC) and Financial Industry Regulatory Authority (FINRA) rules mandate specific reviews and reports that involve regular assessments of risk. This expectation has also been consistently articulated in various SEC Commissioner and senior staff speeches, both before and since the financial crisis of 2008.[6]

In various forms, assessing compliance risk is also codified in various FINRA rules that require securities firms to conduct annual or regular reviews that test a firm's compliance with securities laws and specific areas of risk, document the results of that testing in a report and identify any modifications that were or will be made based on the testing results.[7] For example, FINRA Rule 3110 requires each member to conduct a review, at least annually, 'reasonably designed to assist the member in detecting and preventing violations of, and achieving compliance with, applicable securities laws and regulations, and with applicable FINRA rules.' These inspections and reviews must be reduced to a written report and should include testing and verification of the member's policies and procedures (including supervisory policies and procedures) in specific risk areas.[8] FINRA Rule 3120, in turn, requires firms to submit to senior management, at least annually, a report detailing the firm's system of supervisory controls, the summary of the test results and significant identified exceptions, and any additional or amended supervisory procedures created in response to the test results. The CRA process sits apart from — but should incorporate — testing results, findings and priorities that are identified during these required reviews.

OVERCOMING OBSTACLES: PRACTICAL GUIDANCE FOR DEVELOPING A CRA

Assessing and protecting against risk is, of course, not new. The CRA process quantifies and formalises this effort using a defined and structured methodology and metrics to systematise the vital but necessarily subjective process of predicting, anticipating and seeking to avoid pitfalls. Today, many business executives at financial institutions accept risk and compliance initiatives like CRAs as necessary and — in fact — desirable components of an effective risk management and supervision scheme. With a bit of marketing and involving business heads at every stage of the process, risk and compliance professionals can bring front-line business owners onboard to make the CRA process even more meaningful. In fact, it should be emphasised that the CRA process should be owned by the business and only facilitated by the second-line support functions (such as risk and compliance). While some business-line personnel may voice concerns that CRA programmes create a roadmap to deficiencies for the regulators, receptive business leaders with a long view recognise the importance of effective CRAs and can be emissaries and proponents both up and down the chain of command. Noting a deficiency that is not adequately mitigated should result in a plan to remediate the deficiency, demonstrating to regulators the solution along with the potential issue. While a CRA must be transparent and complete in order to be effective, business leaders do have some

leeway to name and describe the potential deficiency in a manner that does not send alert signals to an audit or regulatory reviewer. Having a comprehensive process to assess and address risks makes those risks quantifiable, controllable and therefore manageable.

The fundamental steps for developing a CRA are generally accepted as the following: (1) preparing an inventory of risks and conflicts along with rules and regulations where applicable; (2) mapping risks and conflicts to policies, procedures and controls and noting actual or potential deficiencies; (3) scoring the risks mitigated by the controls on a rating priority scale; and (4) developing a plan for remediation and testing. Ultimately, there is no one-size fits all CRA and firms should tailor their CRAs to their businesses, personnel, specific risks and customer base.

Preparing an inventory of risks

As a first step, firms must identify regulatory and legal issues, conflicts, conduct risk and other matters regarding a firm's activities that may create risk to the interests of the firm and/or its clients (the 'inherent risks'). This step is one of the most critical steps to the CRA process and, in preparing an inventory of inherent risks, firms should conduct a comprehensive analysis of applicable rules and regulations. To do this, some firms may recruit the assistance of experts (including external counsel) and industry and peer groups.

Sources for identifying inherent risks may include: (1) compliance data (eg surveillance findings and branch, supervisory control and other review testing results); (2) non-compliance, internal testing/exam data (eg internal audit findings, other internal testing results); (3) external reviews and settlements (eg SEC/FINRA examinations for US Broker Dealers, inquiries, investigations and settlements); (4) customer data (eg customer complaints); (5) business data (eg profit and loss information, new product approval data, complexity of product); and (6) regulatory data (rule changes, significant disciplinary actions or settlements and areas of regulatory focus, priorities or scrutiny).

Methods for identifying inherent risk may include questionnaires that quantify both identified risks and risk control effectiveness. These questionnaires may be completed by compliance coverage officers in cooperation with business heads globally and used to identify potential areas of risk for each officer's coverage area and the effectiveness of corresponding controls. A useful CRA will remain flexible so that there can be a reevaluation of risks and priorities if new risk or issues arise after the initial identification of inherent risks.

Mapping risks and conflicts to policies, procedures and controls

The next step for an effective CRA is to review the processes surrounding the identified risk areas (ie inherent risks) in order to identify the policies, procedures and controls that are in place to mitigate and control the inherent risks (the 'risk controls'). Data inputs for identifying the controls that are in place may include the following: (1) policies and procedures; (2) training; (3) surveillance and monitoring; (4) testing; and (5) regulatory reporting.

The trap to avoid here is over-reliance upon the same controls for several inherent risks. Effective supervision is a given, broad and over-general control which, while important, should not be the predominant control for any risk. Similarly, the employee handbook or general compliance manual should be only some of many controls in place to ensure employees are aware of the rules, risks and consequences of negligent or improper activity.

Similarly, internal and independent audits and regulatory examinations, all of which can contribute to effective controls, should not substitute for specific monitoring,

testing and surveillance to control risks. The initiation of a CRA is a genuine opportunity to initiate new (and dust off and update old and unused) controls that serve the valuable function of mitigating the risks which are by nature involved in financial service transactions.

In evaluating risk controls, firms should ask the following key questions:

- Is the control designed effectively? This question requires an exploration of: How reliable is the control? Will the control identify exceptions in each necessary instance? What business lines or systems are covered by the control? Can the control be easily circumvented?
- Does the control operate effectively? This question requires an exploration of: How well does the control perform in practice? Does it function as intended? Are there periodic assessments of controls? Are updates and improvements to controls reflected (to show progress toward reducing risk)?

Prioritising risk areas

Based on the analysis of inherent risks and risk controls described above, firms should: (1) assess where compliance efforts and resources should be focused (the 'residual risks'); and (2) prioritise these risk areas.[9] In prioritising risk areas, there are no regulatory requirements to use a particular ranking or rating system (*eg* 'low, medium and high' versus 'one-to-five'). As a general matter, an effective rating system should reasonably ensure that conclusions are consistent and based on a logical, carefully documented rationale. If ratings are over-ridden after initially assigned, the basis for the over-ride should be documented.

Developing a plan for remediation and testing

Based on the risk assessment, firms should develop a plan to remediate weak controls and areas to be tested. New controls should be implemented throughout the year, while areas of weakness and new risks may be identified through the testing process and evaluation of new business initiatives. Although it may seem obvious, when developing a plan for remediation and testing, it is crucial to be realistic about what can actually be accomplished within the given time period. The compliance commandment 'thou shalt not create procedures and policies more stringent that the actual regulation unless compliance is assured' is nowhere more important than in CRA.

Timing of risk assessment

There is no regulatory-mandated timeframe for conducting a risk assessment review. Some firms may incorporate the risk assessment process into the firm's annual reviews required by FINRA and other rules (described above in the section on 'Regulatory backdrop for implementing CRAs'). Other firms may meet quarterly or less often to discuss risk. Still others have unscheduled impromptu risk meetings or add 'risk' as an agenda item to another meeting, such as a board meeting or compliance staff meeting. Ideally, the risk assessment process should occur on a regular basis and as triggering events occur.

A triggering event may include entering into a new line of business, launching new products, finding a problem in-house, or learning of a recent significant legal or regulatory action against a similarly-situated firm. For each triggering event, a firm should assess the risks and conflicts that might arise and ensure that the firm has a process in place to address those potential risks and conflicts.

Benefitting from experience

The CRA model, used effectively, can become even more meaningful in the evolution of a firm's overall risk controls. For firms just

starting down the CRA path, it may be challenging to identify all of the inherent risks and even to identify the controls in place to mitigate those risks. A few resources to begin the task of building a firm's CRA for the first time include: (1) the firm's own disciplinary record (exceptions noted in regulatory exams, inquiries, complaints and internal disciplinary matters); (2) a review of regulatory sanctions against other similar firms; and (3) checklists published by industry groups and regulators, such as the FINRA Written Supervisory Procedure Checklist.[10] In listing controls, firms may initially find that 'employee manual,' 'e-mail review' and 'annual compliance training' may be mitigating controls when nothing else is squarely on point. A vital component of the effective application of the CRA process is to take a critical look at those controls already in place, or those added to mitigate risks that have been identified during the CRA process. As the CRA process matures within a firm, a separate step should be regularly undertaken to take a fresh look at each identified risk and each control to see if they suggest any additional inherent risks, any controls that are already in place or any controls that should be added. Using this process pro-actively to identify the need for additional safeguards can move the CRA process from a 'check the box' effort to a truly meaningful exercise. At the same time, it is important to be realistic about what can be achieved once risks are identified. To this end, firms should be careful not to create a 'laundry list' of issues that cannot reasonably be remediated within the review cycle. Instead, they should adopt a balanced approach for identifying risks and dealing with them. Firms that are regulated in the United States by FINRA also should keep in mind that issues they identify may need to be self-reported pursuant to FINRA Rule 4530(b) if these issues meet that rule's reporting threshold.[11]

CONDUCT RISK

In order to be effective, CRAs must incorporate risks associated with both intentional and inadvertent conduct. Although the term 'conduct risk' increasingly has become a priority for regulators over the years and a buzzword among financial services professionals, there is no official or commonly accepted definition of 'conduct risk.'[12] Nonetheless, conduct risk is broadly understood as any action or inaction by firm personnel that could lead to unfair client outcomes, impact the integrity of the markets, or otherwise compromise the firm's reputation or financial position. Conduct risk incorporates matters such as how customers are treated, staff actions calculated for the deliberate purpose of affecting remuneration and how firms deal with conflicts of interest.[13]

Key drivers of conduct risk

Conduct risk assessments target key drivers of behaviour and cultural factors, not just formal policies and controls, with a particular focus on: (1) firm culture ('tone at the top'); (2) conflicts of interest (created by business models and strategies); and (3) 'people risk' (created by behavioural incentives or disincentives, in particular, compensation and disciplinary practices) in decidedly that order, as noted above.

Defining 'firm culture'

'Firm culture' has been described as 'the set of explicit and implicit norms, practices, and expected behaviors that influence how firm executives, supervisors and employees make and implement decisions in the course of conducting a firm's business.'[14] In its 2016 Regulatory and Examinations Priorities Letter, FINRA identified a focus on culture, conflicts of interest and ethics among its top priorities.[15] FINRA stated that it will formalise its assessment of firm culture to better understand how it impacts compliance and

risk management and that its understanding of firm culture will inform its evaluation of individual firms and the regulatory resources that FINRA devotes to examining them. In particular, FINRA outlined five indicators for assessing a firm's culture: (1) whether control functions are valued within the organisation; (2) whether policy or control breaches are tolerated; (3) whether the organisation proactively seeks to identify risk and compliance events; (4) whether immediate managers are effective role models of firm culture; and (5) whether sub-cultures that may not conform to overall corporate culture are identified and addressed.[16]

Conflicts of interest

For over a decade, the importance of identifying and managing risks presented by conflicts of interest has been a priority for the securities regulators. As one prominent regulator has noted, every financial firm faces potential conflicts of interest in its business. While conflicts are 'inherent in the financial services industry … [t]he historical success of the financial services industry has been in properly managing these conflicts, either by eliminating them when possible, or disclosing them.'[17]

Conflicts of interest exist both across and within each firm's business lines. Effective practices in managing conflicts include: (1) systematically identifying conflicts on an ongoing and periodic basis and creating a 'conflicts inventory'; and (2) periodic testing and risk assessments of the conflicts management framework and controls that are designed to address the issues in the conflicts inventory.[18]

'People risk'/behavioural incentives or disincentives

'People risk' may be mitigated or exacerbated by certain behavioural incentives or disincentives. Compliance culture, introduced and regularly reinforced by all levels up to senior management, compliance and training, may well be the most effective control for 'people-' or conduct risk. The manner in which personnel are compensated can exacerbate or mitigate risk.[19] In addition to compensation, the manner in which firms discipline employees is an important tool in deterring improper behaviour and influencing 'people risk.'

Identifying inherent risks presented by conduct risk

In order to identify inherent risks influenced by conduct risk, firms should assess both the general internal and external conflicts that may arise as a result of their respective business models and conflicts specific to particular business lines or departments. General categories of conflicts of interest that may be included in the conflicts inventory include: (1) firm versus client conflicts (eg the firm recommends proprietary product or products for which the firm receives higher fees than other products); (2) client versus client conflicts (eg the firm has multiple clients interested in acquiring the same assets or multiple clients with competing interests); (3) employee versus client conflicts (eg compensation arrangements or incentives affect whether employees recommend a particular transaction to a client); and (4) employee versus firm conflicts (eg an employee engages in outside business activities that could conflict with the interests of the firm).

Conflicts specific to particular business lines or departments will depend on the specific activities in which a firm engages, as well as its customer base. For example, if a firm engages in banking and capital markets activities, conduct risk exposure may be raised if the firm serves in multiple roles on a single transaction (eg advises one bidder for a company while financing another, advises on both sides of the same deal, advises a seller while financing a buyer, finances multiple bidders or advises

on the buy or sell side where the firm has an interest in one or more involved parties) without appropriate silos and effective information barriers. If a firm provides research services, conduct risks may be raised if internal and external parties are not prevented from exerting pressure on research analysts to express a particular view in a research report. For example, research may be subject to pressure from investment bankers on behalf of their own interests or those of issuers to initiate coverage, publish reports or change ratings in order to help win or sustain investment banking business. If a firm provides sales and trading services to retail or institutional customers, conduct risks may arise from compensation or sales incentive practices (eg preferencing particular products or services because of their income potential for the firm or registered representative) or breakpoints which may be subject to manipulation.

Mapping conduct risk to policies, procedures and controls

There is no one-size-fits-all approach to managing conduct risk. Key control areas that firms may consider in assessing how conduct risk is managed include, but are not limited to: governance and risk management structure with clear reporting lines and 'owners' with accountability; compensation structures and supervisory reporting lines that do not create improper incentives or allow for improper behaviour; and the adequacy of firm-wide policies and procedures that are designed to address conduct and conflicts of interest.

With regard to governance and risk management structures, specific aspects that may mitigate conduct risk include: (1) heightened supervisory review and vetting of new products, services, business lines, or types of clients); (2) the existence formal escalation procedures and protocol; (3) the code of ethics and conduct; (4) regular training and regular surveillance and testing and formal process for addressing 'red flags'; and (5) the firm's tolerance for bad behaviour, as evidenced by the manner in which the firm disciplines employees for improper conduct.

For compensation, examples of controls that address conduct risk include compensation structures that minimise incentives to favour one type of product over another and avoid thresholds that enable firm personnel to increase their compensation disproportionately through an incremental increase in sales. Some firms also may consider adherence to compliance in performance metrics for both employees and their supervisors.

Finally, with regard to the adequacy of firm-wide policies and procedures that are designed to address conduct and conflicts of interest, areas that may be addressed include: (1) adequacy of information barriers between business lines (for conflicts purposes and to safeguard confidential client or firm information); (2) limitations on outside business interests and activities, personal trading and entertainment to address conflicts, conduct risk and reputational concerns; and (3) mandatory vacation policies (eg to detect 'rogue' activity).

Adding conduct risk to a CRA programme requires a more nuanced and tailored assessment of a firm's particular risks, business lines and client base. It is, however, an important element because many of the recent multi-million and multi-billion dollar settlements have not involved technical rule violations, but rather practices involving fraudulent or misleading conduct.

CONCLUSION

The CRA process can be a meaningful, utilitarian and genuinely beneficial risk identification and management tool. This paper has outlined some key elements and practical considerations for conducting a CRA. While implementing a CRA may seem like a daunting and time-consuming effort, it can pay off in terms of mitigating

fines and losses, safeguarding the reputation of the firm and avoiding customer harm. By better identifying compliance risks and managing the drivers of these risks and behaviour, a CRA not only helps firms to reduce the occurrence of conduct events, but also enhances the way that firms do business.

References and Notes

(1) Stefanyszyn, D. and Detchemendy, J. Examiners, Federal Reserve Bank of St. Louis (2013) 'Conducting consumer compliance risk assessments — Examiner insights,' Outlook Live Webinar, 20th August, available at: https://consumercomplianceoutlook.org/outlook-live/2013/conducting-consumer-compliance-risk-assessments/ (accessed 20th January, 2017) (hereinafter 'Federal Reserve Webinar'). Generally speaking, 'compliance risk' constitutes the risk of legal or regulatory sanctions or financial loss that may be suffered as a result of the failure to comply with laws, regulations, rules and related market standards applicable to a firm.

(2) Federal Reserve Supervisory Letter SR 08-08, 16th October, 2008.

(3) *Idem* at §III — Compliance Monitoring and Testing (note 8).

(4) More recent guidance from banking regulators provides standards for the design and implementation of a risk governance framework. See 'Enhanced prudential standards for bank holding companies and foreign banking organizations', 79 Fed. Reg. 17240, 24th March, 2014 (discussing standards for risk management requirements, including establishing a risk committee, for large US bank holding companies and foreign banking organisations); 'Office of the Comptroller of the Currency guidelines establishing heightened standards for certain large insured national banks, insured federal savings associations, and insured federal branches; Integration of regulations', 79 Fed. Reg. 54518, 11th September, 2014 (adopting guidelines establishing minimum standards for the design and implementation of a risk governance framework).

(5) 'An effective compliance management system commonly has four interdependent control components: Board and management oversight; Compliance program; Response to consumer complaints; and Compliance audit. When all of these four control components are strong and well-coordinated, a supervised entity should be successful at managing its compliance responsibilities and risks.' CFPB Supervision and Examination Manual, October 2012, p. CMR2.

(6) See, for example, Richards, L. (2004) 'Remarks before the National Society of Compliance Professionals 2004 National Membership Meeting', 28th October, 2004, Office of Compliance Inspections and Examinations (OCIE), Securities and Exchange Commission, (stating that all firms must be proactive in identifying risk areas and in endeavoring to mitigate or eliminate those risks, including identifying conflicts of interest that might incentivize illegal and unethical behaviour and advising securities markets participants to '[r]eview your firm's operations and ensure that key risk areas are covered by strong internal controls… [t]est procedures regularly, improve them, question frequently whether they can't be better'); Gadziala, M. A. (2005) 'Remarks before the NYSE Regulation First Annual Securities Conference', 23rd June, OCIE, Securities and Exchange Commission (noting that a 'comprehensive analysis by a firm typically includes the identification of all existing and potential legal and compliance risks, assignment of the level of inherent risk (high, medium low), and identification and rating of controls or mitigants'); and di Florio, C.V. (2012) 'Remarks at the Compliance Outreach Program', 31st January, OCIE, Securities and Exchange Commission (noting that '[s]trong risk management controls, including a solid compliance program, are a key responsibility of everyone in a regulated entity, but the right culture and tone at the top are especially the responsibility of senior management and the board').

(7) See, for example, FINRA Rule 3110 (Annual Review and Report); FINRA Rule 3120 (Supervisory Control System

and Annual Report); FINRA Rule 3130 (Annual CEO Certification of Compliance and Supervisory Processes); and FINRA Rule 3310 (Anti-Money Laundering Compliance Program).

(8) These areas are: safeguarding of customer funds and securities; maintaining books and records; supervision of supervisory personnel; transmittals of funds (eg wires or cheques, etc.) or securities from customers to certain entities or accounts; and changes of customer account information, including address and investment objectives changes and validation of such changes.

(9) 'Inherent risk' has also been generally defined as the risk of error if there were absolutely no controls in place, whereas 'residual risk' is the level of risk present after effective controls are accounted for, such as policies, secondary reviews, etc. See Federal Reserve Webinar, at note 6.

(10) This checklist is available on FINRA's website, at: http://www.finra.org/industry/registration-forms (accessed 20th January, 2017).

(11) As set forth in Supplementary Material .01 to FINRA Rule 4530, with respect to violative conduct by a member firm, FINRA expects a member to report only conduct that has widespread or potential widespread impact to the member, its customers or the markets, or conduct that arises from a material failure of the member's systems, policies or practices involving numerous customers, multiple errors or significant dollar amounts.

(12) A 2016 survey of financial services firms found that 64 per cent did not have a working definition of 'conduct risk'. That number is down from 81 per cent in the previous year and still represents a preponderance of firms. Thomson Reuters (2016) 'Thomson Reuters survey of conduct risk', January. One prominent firm defines conduct risk as '[d]etriment caused to our customers, clients, counterparties, or the Bank and its employees through inappropriate judgment in execution of business activities.' Barclays PLC Annual Report, 2014.

(13) See, for example, Thomson Reuters (2015) Conduct Risk Report 2014/15; Walshe, J. (2014) 'Conduct risk: An overview,' Thomson Reuters, 19th March.

(14) FINRA (2016) '2016 Regulatory and examination priorities letter', 5th January, available at: http://www.finra.org/sites/default/files/2016-regulatory-and-examination-priorities-letter.pdf (accessed 20th January, 2017). In February 2016, FINRA sent a targeted exam letter to select firms regarding how firms establish, communicate and implement cultural values, and whether cultural values are guiding business conduct. The letter is available at http://www.finra.org/industry/establishing-communicating-and-implementing-cultural-values (accessed 20th January, 2017).

(15) *Idem*.

(16) In 2008, FINRA emphasised the importance of the 'tone at the top,' noting that 'even the most rigorous internal controls and risk management procedures can fail if they are not effectively enforced and the effectiveness of that enforcement is directly related to the 'tone at the top.' FINRA Regulatory Notice 08-18, April 2008.

(17) SEC Director of Enforcement, Cutler, S. M. (2003) 'Remarks before The National Regulatory Services Investment Adviser and Broker-Dealer Compliance/Risk Management Conference', 9th September. FINRA has noted that 'conflicts of interest represent a recurring challenge that contribute to compliance and supervisory breakdowns which can lead to firms and registered representatives, at times, compromising the quality of service they provide to clients.' Conflicts of Interest Review – Compensation and Oversight, August 2015, available at: https://www.finra.org/industry/conflicts-interest-review-compensation-and-oversight (accessed 20th January, 2017).

(18) See, generally, FINRA Report on Conflicts of Interest, October 2013 (providing conflicts of interest examples from firms' enterprise-level conflicts policies).

(19) *See idem*.